Filed 12/31/2024 5:23 PM
Accepted: 1/2/2025 8:42 AM
Tammy Robinson
District Clerk
Taylor County, Texas
Monica Mendoza

CASE NO. 13479-D

KYLEE HOPPER, *on behalf of herself and all others similarly situated*, Plaintiff, v. MCMURRY UNIVERSITY, Defendant.	IN THE DISTRICT COURT TAYLOR COUNTY, TEXAS Taylor County - 350th District Court _____ JUDICIAL DISTRICT

PLAINTIFF'S ORIGINAL CLASS ACTION PETITION

Plaintiff Kylee Hopper ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this class action against Defendant McMurry University ("Defendant"). The allegations set forth in this Petition are based on Plaintiff's personal knowledge as to her own actions and experiences, and upon information and belief and further investigation of counsel.

SUMMARY OF ACTION

1. This action arises from Defendant's recent data breach ("Data Breach") resulting from its failure to implement reasonable, industry standard data security practices.

2. Founded in 1923, Defendant is a United Methodist university with more than 1100 students enrolled per year.[1]

3. Plaintiff brings this Petition against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' sensitive information that it collected and maintained as part of its regular business practices, including, but not limited to, names and Social Security numbers ("Private Information") of its current and former students and employees.

[1] https://mcm.edu/about-mcmurry/.

4. Defendant received Plaintiff's and Class Members' Private Information in its provision of its education services to its students for the benefit of Plaintiff and Class Members.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. According to the letter that Defendant sent to Class Members, Defendant admits an unauthorized actor unlawfully accessed certain personal information from its network.

7. The information compromised in the Data Breach included Private Information of individuals whose Private Information was maintained by Defendant, including Plaintiff.

8. Upon information and belief, the Private Information implicated in the Data Breach included names and Social Security numbers.

9. The Data Breach was a direct result of Defendant's failure to implement the adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class members' Private Information which it was obligated to protect.

10. The mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

11. Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of

Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

12. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

13. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Private Information of Plaintiff and Class Members.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

15. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft. As

a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

16. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' Private Information was targeted, accessed, and misused, including by dissemination on the Dark Web.

17. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

18. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of their Private Information; and (f) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

19. Through this Petition, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

20. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of third-party beneficiary contract, and (iii) unjust enrichment.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

22. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

23. Plaintiff further believes her Private Information, and that of proposed Class Members, was subsequently sold on the Dark Web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff experienced fraudulent misuse of her compromised information that would support this well-founded belief.

PARTIES

24. Plaintiff is, and at all relevant times was, a resident and citizen of Abilene, Texas.

25. Defendant is a Texas corporation with its principal place of business located at 1400 Sayles Blvd., Abilene, Texas 79697. Defendant may be served with process through its registered agent for service of process, Lisa L. Williams. 1400 Sayles Blvd., Abilene, TX 79697.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this controversy because the contract between Defendant and its students, made for the benefit of Plaintiff and Class Members, was

established in Texas. Moreover, Defendant's failure to adequately safeguard Plaintiff and Class Members' data, *i.e.*, Defendant's negligent conduct, occurred in Taylor County, Texas. Plaintiff has been damaged in a sum within the jurisdictional limits of this Court.

27. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in Taylor County, Texas.

28. Venue is proper in this county under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in this county.

29. Upon information and belief, more than two-thirds of the Class are citizens of Texas.

30. Pursuant to Texas Rule of Civil Procedure 47, Plaintiff seeks monetary relief over $1,000,000 for the Class.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims

31. Upon information and belief, Plaintiff's individual damages are less than $75,000.

32. At all relevant times, Defendant knew it was storing sensitive Private Information and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

33. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

34. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

35. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of

open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[2]

36. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[3]

37. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[4]

38. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's students and employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

39. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

---

[2] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[3] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[4] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[5]

40. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained Private Information about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect Plaintiff's and Class Members' Private Information

41. Defendant agreed to and undertook legal duties to maintain the personal information entrusted to it by and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTC Act"). Under state and federal law, businesses like Defendant have duties to protect its current and former students' and employees' Private Information and to notify them about breaches.

42. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiff and Class Members.

43. On June 20, 2024, Defendant became aware of unusual activity that disrupted access to certain of its systems. According to Defendant, upon discovery of the Data Breach, it promptly began an investigation. The investigation subsequently revealed certain personal

[5] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

information was acquired without authorization by an unknown actor on or about June 18 to 20, 2024. Defendant undertook a comprehensive review of the potentially impacted data to identify the individuals and data involved, which concluded on November 15, 2024.

44. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect Plaintiff's and Class Members' Private Information.

C. Plaintiff's Experience

45. Plaintiff received a Notice Letter from Defendant notifying her of the Data Breach. The Notice Letter is dated December 23, 2024.

46. The Notice Letter advised Plaintiff that her name and Social Security number were accessed without authorization on or about June 18 to 20, 2024.

47. On information and belief, Plaintiff's Private Information has been published on the Dark Web, as that is *modus operandi* of cybercriminals of the type who perpetrated the Data Breach.

48. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. she has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

49. Plaintiff is not aware of ever being part of a data breach involving her Private Information and is concerned that it and other private information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft.

50. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing

credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

51. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Plaintiff is also concerned that her privacy has been violated and fears her Private Information will be used to commit identity theft.

52. Plaintiff has spent time and anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

53. Plaintiff greatly values her privacy and would not have provided her Private Information and undertaken Defendant's services if she had known that her Private Information would be maintained using inadequate data security systems.

D. Plaintiff and Class Members Suffered Damages

54. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitoring their statements, bills, records, and credit and financial accounts; 2) changing login and password information on any sensitive account even more frequently than they already do; 3) more carefully screening and scrutinizing phone calls, emails, and other communications to

ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) searching for suitable identity theft protection and credit monitoring services, and pay to procure them.

55. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

56. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

57. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[6]

58. Plaintiff and the Class Members have also been injured by Defendant's unauthorized disclosure of their confidential Private Information.

59. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect Plaintiff and Class Member's Private Information.

COMMON INJURIES AND DAMAGES

[6] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

60. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

61. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

A. The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

62. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

63. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

64. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

65. The Dark Web is an unindexed layer of the Internet that requires special software or authentication to access.[7] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[8] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

66. A sophisticated black market exists on the Dark Web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[9] The digital character of Private Information stolen in data breaches lends itself to Dark Web transactions because it is immediately transmissible over the Internet and

[7] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[8] *Id.*
[9] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[10] As Microsoft warns "[t]he anonymity of the Dark Web lends itself well to those who would seek to do financial harm to others."[11]

67. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

68. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

[10] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[11] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[12] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[14]

71. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[15]

72. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[16] Defendant did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

---

[13] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[14] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[15] *See* https://www.fbi.gov/news/stories/2019-Internet-crime-report-released-021120.

[16] *Id.*

73. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

74. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

75. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

76. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[17]

77. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1)

[17] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[18]

78. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[19]

79. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

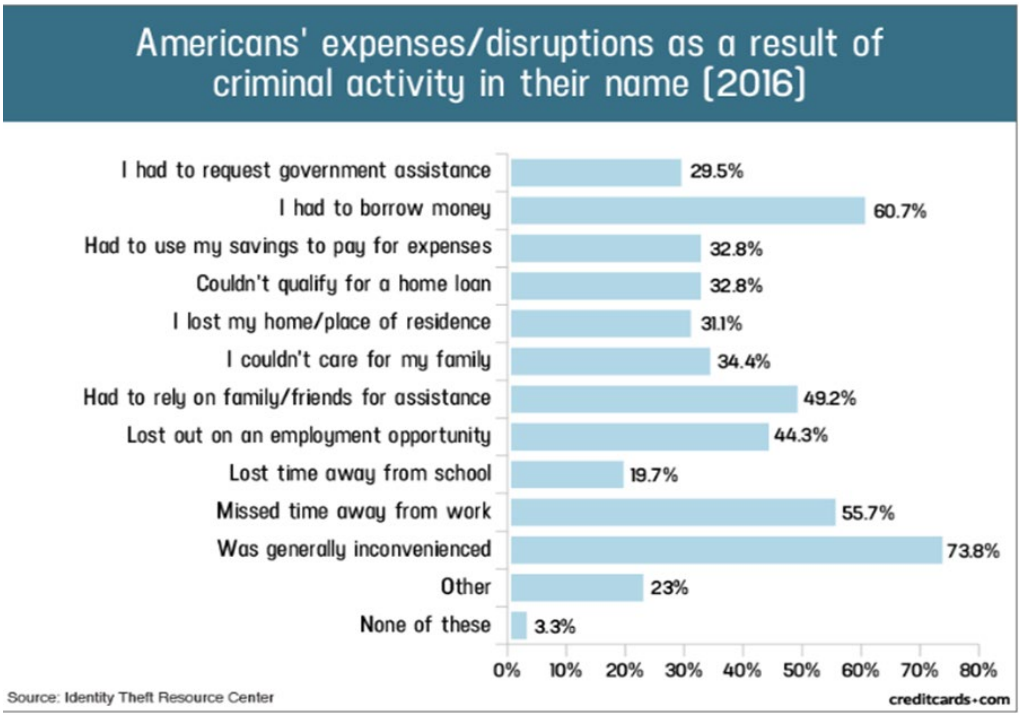
80. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been

[18] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[19] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

lost.

81. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

82. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[20]



83. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time

[20] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

to repair the damage to their good name and credit record."[21] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

C. Diminution of Value of the Private Information

84. Private Information is a valuable property right.[23] Its value is axiomatic, considering the value of "Big Data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

85. Private Information can sell for as much as $363 per record according to the Infosec Institute.[24]

86. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[25] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

[21] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf.
[22] *See* https://www.identitytheft.gov/Steps.
[23] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[24] *See* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[25] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

broker who in turn aggregates the information and provides it to marketers or app developers.[26, 27] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[28]

87. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

88. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has offered one year of complimentary identity theft protection. Furthermore, this is a tacit admission that its failure to protect their Private Information has caused Plaintiff and Class Members great injuries.

89. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for services, as opposed to automatically enrolling all victims of this Data Breach.

90. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make

[26] https://datacoup.com/.
[27] https://digi.me/what-is-digime/.
[28] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

91. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

92. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[29] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

93. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

94. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

E. Injunctive Relief is Necessary to Protect Against Future Data Breaches

95. Moreover, Plaintiff and Class Members have an interest in ensuring that Private

[29] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

96. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they have suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information —which remains in Defendant's possession—and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

F. Lack of Compensation

97. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their

lives as a direct and foreseeable consequence of this Data Breach.

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

99. Further, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

100. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

101. In addition, Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach.

102. Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to fraud, embarrassment, and depriving them of any right to privacy whatsoever.

103. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and did not timely notify all victims. They have yet to offer an explanation or purpose for the delay. This delay violates notification requirements and increases the injuries to Plaintiff and the Class.

CLASS ALLEGATIONS

104. Pursuant to Rule 42 of the Texas Rules of Civil Procedure, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach ("Class").

105. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

106. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

107. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted in the Data Breach. The Class is apparently identifiable within Defendant's records, as Defendant has already identified these individuals (as evidenced by sending them Notice Letters).

108. Commonality and Predominance: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information

of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

These common issues predominate over any issues affecting only individual members of the Class because the parties will spend the overwhelming majority of their time and effort litigating these

issues,

109. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each Class Member.

110. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

111. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

112. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the

adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

113. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

114. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

115. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

116. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may

continue to act unlawfully as set forth in this Petition.

117. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

118. Plaintiff restates and realleges paragraphs 1 through 117 above as if fully set forth herein.

119. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

120. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

121. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

122. Defendant's duty also arose from Defendant's position as a university. Defendant holds itself out as a trusted provider of education, and it thereby assumes a duty to reasonably protect the information of its students and employees and their dependents. Indeed, Defendant, as aa university collecting the sensitive Private Information of its current and former students and

employees and their dependents, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

123. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student and employee information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to timely notify Plaintiff and Class Member about the Data Breach.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

125. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

126. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its

students and employees and their dependents.

127. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

128. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

130. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in

the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their Private Information;

j. The erosion of the essential and confidential relationship between Defendant – as a business – and Plaintiff and Class Members as students or employees.

131. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

132. Plaintiff restates and realleges paragraphs 1 through 117 above as if fully set forth herein.

133. Plaintiff and Class Members directly contracted with Defendant as students or employees.

134. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving education services provided by Defendant, or employment with Defendant.

135. Plaintiff and Class Members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

136. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

137. Plaintiff and the Class Members accepted Defendant's offers by disclosing their Private Information to Defendant or its third-party agents in exchange for medical services.

138. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

139. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

140. After all, Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

141. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

142. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

143. In these and other ways, Defendant breached its implied contract with Plaintiff and the Class.

144. Defendant's material breaches were the direct and proximate cause of Plaintiff' and Class Members' injuries (as detailed *supra*).

145. And, on information and belief, Plaintiff' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

146. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

147. Plaintiff restates and realleges paragraphs 1 through 117 above as if fully set forth herein.

148. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

149. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

150. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and

has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

151. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

152. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

153. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendant or obtained services from Defendant.

154. Plaintiff and Class Members have no adequate remedy at law.

155. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

156. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of the benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information in the form of experiencing an in increase in spam calls, texts, and/or emails; (viii) their Private Information being disseminated on the Dark Web; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

157. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. An Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. Injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to pay out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment and post-judgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: December 31, 2024.

Respectfully Submitted,

By: /s/ *Roger Mandel*
Roger Mandel (Texas Bar No. 12891750)
JEEVES MANDEL LAW GROUP, PC
2833 Crockett St., Ste. 135
Fort Worth, TX 76107
Tel: (214) 253-8300
rmandel@jeevesmandellawgroup.com
khill@jeeveslawgroup.com

Jeff Ostrow (*pro hac vice* application forthcoming)
KOPELOWITZ OSTROW PA
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
ostrow@kolawyers.com

Counsel for Plaintiff and the Proposed Class

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Roger Mandel on behalf of Roger L. Mandel
Bar No. 12891750
rmandel@jeevesmandellawgroup.com
Envelope ID: 95764506
Filing Code Description: Letter
Filing Description: RequestforIssuanceHooper v McMurry
Status as of 1/2/2025 8:44 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Kay Hill		khill@jeeveslawgroup.com	12/31/2024 5:23:45 PM	SENT
Roger Mandel		rmandel@jeevesmandellawgroup.com	12/31/2024 5:23:45 PM	SENT